

Applicant : Satyendra Yadav
Serial No.: 10/066,140
Filed: February 1, 2002
Page : 15 of 23

Attorney's Docket No.: 10559-755001/P13653
Assignee: Intel Corporation

REMARKS

Claims 1-35 are pending, with claims 1, 13, 22, 24, 26, and 31 being independent. Claim 31 has been amended. No new matter has been added. Reconsideration and allowance of the above-referenced application are respectfully requested.

Claims 1-35 stand rejected under 35 U.S.C. 102(e) as allegedly being anticipated by U.S. Patent No. 6,996,843 to Moran. This contention is respectfully traversed.

Moran describes an, "intrusion detection system [that] comprises an analysis engine configured to use continuations and apply forward- and backward-chaining using rules." See Moran at Abstract. "Continuations are [...] the representation of the state of a stopped process that allows the computation to be resumed (continued)." See Moran at col. 38, lines 37-39. In addition, "Two categories of rule-based systems are those that use forward-chaining and those that use backward-chaining. Systems that use forward-chaining (602) start with each incoming fact (604) and generate all inferences (606) resulting from the addition of that fact to the knowledge base (608), thereby producing all conclusions that are supported by the available facts. Systems that use backwards-chaining (610) start with a

Applicant : Satyendra Yadav
Serial No. : 10/066,140
Filed: February 1, 2002
Page : 16 of 23

Attorney's Docket No.: 10559-755001/P13653
Assignee: Intel Corporation

goal (614) and search for facts that support that goal, producing a structure of subgoals (612).” See Moran at col. 38, line 61 to col. 39, line 3.

These techniques of Moran do not anticipate the subject matter of the present application. Independent claim 1 recites, “receiving requests for network communication services from an invoked application; selectively designating each of the received requests as authorized or unauthorized based on an application-specific network policy; and monitoring inbound network communications, based on the authorized requests, to detect an intrusion.” (Emphasis added.) Inexplicably, the rejection of claim 1 omits the above underlined portions of the claim when paraphrasing the claim language. Since the rejection ignores elements of the claim, the rejection is clearly insufficient, and should be withdrawn.

Furthermore, the cited portions of Moran do not describe the claimed subject matter. For the claimed receiving, the cited portion of Moran (col. 7, lines 27-32) states:

Computer network 202 also includes a Internet access server 206 configured to enable users of host computer systems connected to the computer network 202 to access the Internet and in particular to access web

Applicant : Satyendra Yadav
Serial No.: 10/066,140
Filed: February 1, 2002
Page : 17 of 23

Attorney's Docket No.: 10559-755001/P13653
Assignee: Intel Corporation

pages via the World Wide Web by sending and receiving
hypertext transfer protocol (HTTP) transmissions.

For the claimed selectively designating, the cited portion of
Moran (col. 7, lines 34-38) states:

Firewall 208 may be either a firewall, or a router
with firewall functionality, configured to route
authorized users to Internet access server 206 and to
detect and route unauthorized users to the trap system
described below.

This clearly indicates that the users are authorized or
unauthorized, and says nothing about how users are found to be
in either category. Moreover, the cited portions of Moran say
nothing about selectively designating each of the received
requests (being requests for network communication services
received from an invoked application) as authorized or
unauthorized based on an application-specific network policy.

For the claimed monitoring, the cited portion of Moran
(col. 9, lines 24-33) states:

In analysis after the fact, however, the data present
must be treated as suspect. The data may include
forgeries planted by the attacker to mislead the
analysis. Preferably, the inventive system deals with
the unknown reliability of the data by examining
redundant and related sources, and then checks for

Applicant : Satyendra Yadav
Serial No.: 10/066,140
Filed: February 1, 2002
Page : 18 of 23

Attorney's Docket No.: 10559-755001/P13653
Assignee: Intel Corporation

inconsistencies and supporting detail. The data is then scored on the basis of its consistency, difficulty of forgery, and likelihood of its being tampered with by an attacker (based on known and projected activity of current attackers).

The rejection provides no explanation of how this portion of Moran can be considered to relate back to the earlier cited portions, or how the described analysis of after the fact data using consistency checks to identify suspect data can in any way be considered to teach monitoring inbound network communications, based on the authorized requests, to detect an intrusion.

Rather, it appears that the Office Action merely paraphrases (incorrectly) the claim language, without considering the interrelationship of the claimed elements, and then cites unconnected portions of Moran without any explanation of how they can be considered to teach the claimed subject matter. Thus, the rejection of independent claim 1 is clearly both legally and factually deficient, and should be withdrawn.

The rejections of independent claims 13, 22 and 26 are deficient based on reasoning similar to that for claim 1. In addition, for claims 13 and 26, the Office Action fails to

Applicant : Satyendra Yadav
Serial No.: 10/066,140
Filed: February 1, 2002
Page : 19 of 23

Attorney's Docket No.: 10559-755001/P13653
Assignee: Intel Corporation

address the claimed, "identifying an invoked application", and does not describe how Moran can be considered to teach, "initiating monitoring of network communications for the invoked application using an application-specific intrusion signature in response to one or more unauthorized requests." The cited portion of Moran (col. 8, lines 11-16) states:

Analysis engine 302 utilizes ruleset 306 and an attack signatures database 308, and receives input from sensor controller 310. The sensor controller 310 is in communication with various sensors (in the form of data collection modules) 312, and may pass information to the event database 304.

There is no indication here that the attack signatures database 308 of Moran includes application-specific intrusion signatures. Moreover, nothing in this portion of Moran describes, "initiating monitoring of network communications for the invoked application using an application-specific intrusion signature in response to one or more unauthorized requests." (Emphasis added.) Thus, the rejection of independent claims 13 and 26 is clearly both legally and factually deficient, and should be withdrawn.

With respect to independent claim 22, Moran does not teach, "an application network policy enforcer, which services network

Applicant : Satyendra Yadav
Serial No.: 10/066,140
Filed: February 1, 2002
Page : 20 of 23

Attorney's Docket No.: 10559-755001/P13653
Assignee: Intel Corporation

requests from an application invoked on a machine, identifies the network requests that fail to satisfy an application-specific network policy, and identifies the network requests that satisfy the application-specific network policy; a network traffic enforcer, which blocks inbound network traffic that does not correspond to the network requests identified by the application network policy enforcer as satisfying the application-specific network policy; and an intrusion detector, which responds to the network requests identified by the application network policy enforcer as failing to satisfy the application-specific network policy, and which responds to the inbound network traffic blocked by the network traffic enforcer." (Emphasis added.) Thus, the rejection of independent claim 22 is clearly both legally and factually deficient, and should be withdrawn.

With respect to independent claims 24 and 31, the rejection misstates the claim language and fails to address various elements of the claims. For example, the "means for monitoring blocked traffic to identify an intrusion prelude and to identify abnormal application behavior" (emphasis added) of claim 24 is not addressed in the Office Action. Thus, for at least this reason, the rejection of claim 24 should be withdrawn.

Applicant : Satyendra Yadav
Serial No.: 10/066,140
Filed: February 1, 2002
Page : 21 of 23

Attorney's Docket No.: 10559-755001/P13653
Assignee: Intel Corporation

As another example, the "receiving information about a potential intruder in response to the generated fabricated response" (emphasis added) of claim 31 is not addressed in the Office Action. Nonetheless, claim 31 has been amended to recite, "wherein the detecting comprises detecting communication activities including system scans, port scans, and operating system fingerprinting." See e.g., Specification at ¶ 46. Thus, for at least these reasons, the rejection of claim 31 should be withdrawn.

In view of the above, independent claims 1, 13, 22, 24, 26, and 31 should be in condition for allowance. Dependent claims 2-12, 14-21, 23, 25, 27-30, and 32-35 should be allowable based on the above arguments and the additional recitations they contain. In addition, for many of the dependent claims (as with the independent claims), the Office Action misstates the claim language and cites unconnected portions of Moran, without any explanation of how Moran can be fairly considered to teach the claimed subject matter. These rejections are clearly both legally and factually deficient, and should be withdrawn.

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific issue or comment does not signify agreement with or concession of that

Applicant : Satyendra Yadav
Serial No.: 10/066,140
Filed: February 1, 2002
Page : 22 of 23

Attorney's Docket No.: 10559-755001/P13653
Assignee: Intel Corporation

issue or comment. Because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

It is respectfully suggested for all of these reasons, that the current rejections are overcome, that none of the cited art teaches or suggests the features which are claimed, and therefore that all of these claims should be in condition for allowance. A formal notice of allowance is thus respectfully requested.

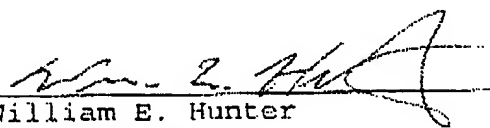
Applicant : Satyendra Yadav
Serial No.: 10/066,140
Filed: February 1, 2002
Page : 23 of 23

Attorney's Docket No.: 10559-755001/P13653
Assignee: Intel Corporation

No fee is believed due with this response. Please apply
any necessary charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: May 8, 2006



William E. Hunter
Reg. No. 47,671
Attorney for Intel Corporation

Fish & Richardson P.C.
PTO Customer No. 20985
12390 El Camino Real
San Diego, California 92130
Telephone: (858) 678-5070
Facsimile: (858) 678-5099

10009146.doc